Quiz 6 Solutions

written by Alvin Wan . alvinwan.com/cs70

Monday, September 26, 2016

This quiz does not count towards your grade. It exists to simply gauge your understanding. Treat this as though it were a portion of your midterm or final exam.

1 Fermat's Little Theorem

1. Prove that if p is prime, $x^a = x^{a \mod (p-1)} \mod p$.

   Solution: Let $a = m(p-1)+n$, where $n = a(\text{mod}(p-1))$ and $m = \lfloor \frac{a}{p-1} \rfloor$. Plug in a, and we have

$$\begin{aligned} x^{m(p-1)+n} &= x^{(p-1)m}x^n \mod p \\ &= (x^{p-1})^m x^n \end{aligned}$$

   By Fermat's Little Theorem, $x^{p-1} \equiv 1 \mod p$. Thus,

$$\begin{aligned} (x^{p-1})^m x^n &= x^n \\ &= x^{a(\text{mod}(p-1))} \end{aligned}$$

2. Solve $2016^{2016^{2016}} \mod 2017$. (Note: 2017 is prime)

   Solution: Per the proof in part a, we have

$$\begin{aligned} 2016^{2016^{2016}} \mod 2017 &= 2016^{2016^{2016} \mod 2016} \mod 2017 \\ &= 2016^{0^{2016} \mod 2016} \mod 2017 \\ &= 1 \mod 2017 \end{aligned}$$

   We can alternatively note that $2016 = -1 \mod 2017$. Since -1 is raised to an even power, the answer is $1 \mod 2017$.

3. Let p be prime. Is $a^p \equiv a (\text{mod } p) \implies a^{p-1} \equiv 1 (\text{mod } p)$ true?

   Solution: False

   First, note that if p is prime, then we *always* have the following $a^p \equiv a (\text{mod } p)$. Second, if $a > 0$, a is not divisible by p, *and p is still prime*, then we *additionally* have that $a^{p-1} = 1 (\text{mod } p)$.

   Although $a^p = a (\text{mod } p)$ is always true when p is prime, $a^{p-1} \equiv 1 (\text{mod } p)$ is not. The latter is true only if we also have that p does not divide a, and $a > 0$.